# ESQUEMAS CRIPTOGRÁFICOS VISUALES

*Luis Hernández Encinas, Fausto Montoya Vitini y Jaime Muñoz Masqué*
Dpto. Tratamiento de la Información y Codificación.
Instituto de Física Aplicada, C.S.I.C. C/ Serrano 133. 28006, Madrid
{luis, fausto, jaime}@iec.csic.es

**Resumen**

Los esquemas criptográficos visuales son protocolos criptográficos que codifican un mensaje formado por una imagen definida por píxeles en vez de codificar un mensaje de texto definido por letras y números. Los esquemas visuales se definen a partir de los esquemas umbrales y han dado lugar al nacimiento de la Criptografía Visual. En este artículo se presentan estos esquemas y se da una visión global del estado del arte en esta rama de la Criptografía: se definen los esquemas visuales umbrales, se introducen los conjuntos de participantes cualificados para recuperar la imagen original, se señalan los problemas de contraste al efectuar la recuperación de la imagen (mensaje) codificada y se aplican estos esquemas a los protocolos de autenticación e identificación.

## 1. INTRODUCCIÓN

Como es bien sabido, el objetivo de la Criptografía consiste en intercambiar de forma segura un mensaje de modo que ninguna persona no autorizada pueda tener acceso a la información contenida en el mismo. El procedimiento utilizado consiste en cifrar el mensaje de modo que lo haga irreconocible para quien no esté autorizado a recuperar el texto original. Los métodos de cifrado más empleados en la actualidad se basan en algoritmos matemáticos que utilizan determinados parámetros, conocidos como claves. La seguridad de tales algoritmos se suele basar en la presunta intratabilidad computacional de un problema matemático (factorización entera, logaritmo discreto, etc.).

En el caso particular de que el mensaje no esté formado por letras y números sino que esté formado por una imagen definida por píxeles blancos y negros, estamos ante otro tipo de criptografía, que se ha dado en llamar Criptografía Visual. Esta nueva criptografía, que no necesita ningún tipo de conocimiento criptográfico para la recuperación de la imagen original, fue propuesta por Naor y Shamir ([NS95]) y desarrollada posteriormente por otros autores (véanse [St95], [ABSS96], [ABSS99] y [BSS99]).

La base de los criptosistemas visuales son los esquemas visuales umbrales, quienes a su vez se fundamentan en una aplicación bien conocida de la criptografía como son los esquemas umbrales (ver [FGHMM97], §8.5). En general, un esquema umbral $t$ de $n$ es un procedimiento criptográfico en el que hay $n$ participantes y que es llevado a cabo por un director, $D$. El director divide un secreto $S$ (que puede ser una clave utilizada para cifrar un mensaje) en $n$ partes o *sombras*, proporcionando, de forma secreta, una sombra a cada uno de los $n$ participantes. La división del secreto en sombras debe hacerse de modo que cualesquiera $t$ participantes puedan determinar el valor del secreto $S$ sin más que compartir las $t$ sombras que poseen; y tal manera que ningún grupo de $t$–1 participantes, o menos, pueda obtener información alguna sobre el valor secreto de $S$.

De forma resumida se puede dar una idea de cómo elaborar un esquema umbral 2 de 2, donde el secreto sea, por ejemplo, una cadena de $m$ bits (ver [HM99]). El secreto original se divide en 2 sombras, de modo para recuperarlo será necesario reunir la información de las 2 sombras. El director podría elegir al azar $m$ bits, que serían la primera sombra, mientras que la segunda la obtendría sin más que sumar módulo 2 cada bit del secreto con cada bit de la primera sombra. Posteriormente proporcionaría de forma secreta las sombras a los participantes, quienes deberían reunir (sumando bit a bit) la información de las sombras que poseen para recuperar el secreto original.

Obsérvese que ninguno de los dos participantes obtiene información alguna acerca de los bits de *S* dado que la primera sombra es aleatoria. Además, la elaboración de las sombras es segura, puesto que la recuperación del secreto original a partir de una de las sombras es una tarea difícil: se deberían probar las $2^m$ posibles valores de la otra sombra.

## 2. ESQUEMAS VISUALES UMBRALES

Un esquema visual umbral *t* de *n* es un procedimiento similar a un esquema umbral *t* de *n*, pero caracterizado por el hecho de que el secreto, *S*, es una imagen formada por píxeles blancos y negros y porque las *n* sombras en que se divide el secreto son otras tantas imágenes con el mismo número de píxeles que la imagen original, es decir, cada uno de los píxeles que forman la imagen original es cifrado dando lugar a *n* versiones modificadas de dicho pixel, una para cada sombra. Además, la recuperación del secreto se lleva a cabo fotocopiando cada una de las sombras sobre una transparencia y luego superponiendo *t* transparencias cualesquiera, teniendo en cuenta que dicho secreto no puede recuperarse con *t*–1 transparencias o menos.

Nótese que para la recuperación de la imagen original no se requiere ningún tipo de conocimiento criptográfico ni el uso de ningún algoritmo. Basta con mirar y "ver" la imagen que resulta al superponer las transparencias.

Un proceso para elaborar un esquema visual umbral 2 de 2, no tan elemental como el presentado en [HM99] y que proporciona mejor resolución en la imagen recuperada, consiste en utilizar, para cifrar cada pixel original, píxeles cifrantes constituidos por 4 subpíxeles, dos blancos y dos negros, ordenados en una matriz $2\times2$, de modo que al superponerlos se obtengan píxeles totalmente negros (cifran un pixel negro) o mitad blancos y mitad negros (cifran un pixel blanco). El procedimiento de cifrado de un pixel original consiste en elegir, de forma aleatoria, una cualquiera de las parejas de píxeles cifrantes mostradas en la figura 1.a (horizontales, verticales o diagonales), según sea el color del pixel original. Dado que en la recuperación de la imagen original los píxeles blancos se recuperan mitad blancos, mitad negros, se produce una pérdida de contraste al comparar la imagen original y la que se recupera.

También puede considerarse para este esquema umbral 2 de 2 la posibilidad de cifrar cada uno de los píxeles originales mediante círculos en lugar de cuadrados. Cada círculo se divide en dos semicírculos (subpíxeles), de modo que uno de ellos será negro y el otro blanco, y tales que el diámetro que los separa formará determinado ángulo con la horizontal (ver figura 1.b). Cuando los dos círculos (girados $\alpha$ y $\beta$ grados) se superponen, el rango de tonos que pueden cubrir van desde el medio gris (representando al pixel blanco) hasta el negro (representando al pixel negro), dependiendo del ángulo de rotación, $\alpha-\beta$, entre los dos semicírculos.

Figura 1. Píxeles cifrados mediante subpíxeles cuadrados $2\times2$ o mediante círculos

Si se elige para cada pixel en cada sombra un ángulo de rotación aleatorio (vigilando el ángulo que se desea para la otra sombra), cada una de las dos transparencias parecerá uniformemente gris, con lo que no se obtendrá ninguna información de la imagen original. Como ejemplo, en la figura 2, se pueden comparar las sombras e imágenes en blanco y negro y en tonos grises de una misma imagen secreta.

Figura 2. Imágenes originales (logotipo del CSIC), sombras e imágenes recuperadas en blanco y negro y en tonos grises

Una nueva extensión de este modelo podría llamarse cifrado visual subliminal pues consiste en utilizar dos imágenes aparentemente inocentes como sombras, por ejemplo, un árbol y un pajarillo, de modo que al superponerlas aparezca la imagen cifrada, que no tiene nada que ver con los dibujos del árbol y el pájaro originales. Para ello se consideran píxeles compuestos por 4 (= $2\times2$) subpíxeles, de modo que un pixel blanco se cifra mediante un pixel con 2 subpíxeles negros y un pixel negro se cifra con un pixel que contiene 3 subpíxe-

les negros. Al superponer las sombras se obtienen píxeles blancos formados por 3 subpíxeles negros y píxeles negros formados por los 4 subpíxeles negros.

## 3. ESQUEMAS CRIPTOGRÁFICOS VISUALES

En los esquemas visuales presentados anteriormente se ha considerado que cada pixel original es cifrado mediante píxeles que están divididos en 2 o en 4 subpíxeles. Sin embargo, para extender los esquemas anteriores, se puede considerar que cada pixel de la imagen secreta se cifra mediante *m* subpíxeles para cada una de las *n* sombras. Este número *m* se denomina *expansión del pixel*. Además, en estos esquemas se estudia también un nuevo factor, conocido como *contraste relativo*, que informa de la pérdida de contraste de la imagen original con respecto a la imagen recuperada al descifrar los píxeles blancos originales, debido a que se obtienen píxeles que no son completamente blancos.

En un esquema visual 2 de *n*, el cifrado de un pixel original en *m* subpíxeles se podría hacer de forma parecida a como se hizo antes, es decir, dividiendo cada uno de los dos píxeles cifrantes en *m* subpíxeles y ennegreciendo algunos de ellos. Sin embargo, esta extensión es más fácil de ejecutar si cada pixel dividido en *m* subpíxeles se representa por una colección de *m* dígitos binarios (0 para los subpíxeles blancos y 1 para los negros). Además, como cada pixel original da lugar a *n* píxeles, uno para cada sombra, conviene utilizar dos matrices de tamaño $n \times m$ para describir el esquema, una para los píxeles blancos, $C_0$, y otra para los píxeles negros, $C_1$. En esta situación, el algoritmo para cifrar un pixel en un esquema criptográfico visual 2 de *n* con expansión de pixel *m* es el siguiente:

*Entrada*: un pixel original $P = 0$ ó 1 (blanco o negro).

*Salida*: los *n* píxeles cifrantes de *P* para cada una de las *n* sombras.

1. Seleccionar una permutación aleatoria $\rho$ del conjunto {1, 2, ..., *m*}.
2. $N_P$ es la matriz construida permutando las columnas de la matriz $C_P$ según $\rho$.
3. Desde $i = 1$ hasta *n*, la fila *i* de $N_P$ son los *m* subpíxeles del pixel para la sombra *i*.

Para ilustrar el algoritmo podemos considerar un esquema $t = 2$ de $n = 4$ con expansión de pixel $m = 6$. En este caso, las dos matrices $C_0$ y $C_1$ son las siguientes:

$$C_0 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad C_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Entonces, si se quiere cifrar un pixel negro $P = 1$, se elige una permutación aleatoria del conjunto {1, 2, 3, 4, 5, 6}, por ejemplo $\rho = \{4, 2, 5, 6, 3, 1\}$ y se construye la matriz $N_1$ para este pixel, sin más que permutar según $\rho$ las columnas de la matriz $C_1$:

$$N_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Los $n = 4$ píxeles cifrantes, formados por $m = 6$ subpíxeles cada uno, que codifican el pixel negro original son los que se obtienen de la matriz $N_1$ anterior interpretando cada fila como un pixel cifrante para cada sombra y cada elemento de la fila como el color de cada uno de los subpíxeles que lo forman.

Si lo que se desea es cifrar un pixel blanco ($P = 0$), el proceso sería el mismo pero utilizando la matriz $C_0$ para construir $N_0$.

## 4. ESQUEMAS CRIPTOGRÁFICOS SELECTIVOS

En los esquemas visuales anteriores todos los participantes estaban igualmente cualificados para recuperar la imagen secreta a partir de la sombra que recibían, es decir, en un esquema visual umbral $t = 3$ de $n = 8$, por ejemplo, bastaba con unir las sombras de 3 cualesquiera de los 8 participantes para recuperar la imagen secreta original. Sin embargo, se pueden considerar esquemas visuales con $n$ participantes que no estén caracterizados por el parámetro $t$, es decir, esquemas en los que la recuperación de la imagen original esté determinada no por la unión de las sombras de determinado número fijo de participantes, sino por el hecho de pertenecer o no a un grupo de participantes cualificados. A este tipo de esquema visual umbral lo llamaremos *selectivo*.

De forma más general *un esquema criptográfico visual para un conjunto, P, de n participantes* es un procedimiento criptográfico que permite codificar una imagen secreta, $S$, en $n$ sombras de modo que cada participante del conjunto $P$ recibe una de tales sombras. Si $2^P$ es el conjunto de las partes de $P$, los elementos de determinado subconjunto, $Q$, de $2^P$ son los participantes que pueden recuperar "visualmente" la imagen codificada, si unen sus sombras (participantes cualificados), mientras que el resto de subconjuntos de $2^P$ no tienen acceso a ninguna información de la imagen original ([ABSS96] y [ABSS99]). Nótese que con este esquema criptográfico es posible que no siempre haga falta el mismo número de sombras cada vez que se desee recuperar la imagen. Puede darse el caso que un subconjunto de participantes cualificados esté formado por sólo 2 individuos mientras que otro puede estar formado por 4 participantes diferentes.

Al igual que en los esquemas umbrales anteriores, la recuperación "visual" de la imagen se lleva a cabo fotocopiando las sombras de cada uno de los participantes en una transparencia y superponiéndolas, sin necesidad de que éstos posean conocimientos criptográficos.

La situación que se presenta en un esquema criptográfico selectivo puede ser, más o menos, la del siguiente ejemplo. Se considera un esquema criptográfico visual con $n = 5$ participantes, que denotaremos por {1,2,3,4,5}. En este esquema criptográfico sólo se podrá recuperar la imagen secreta si se forman subconjuntos de participantes que contengan, al menos, a alguno de los siguientes conjuntos de participantes cualificados elementales: {1,5} o {3,4,5}. Por tanto, el conjunto de participantes cualificados, $Q$, es el siguiente:

$Q$ = {{1,5},{1,2,5},{1,3,5},{1,4,5},{3,4,5},{1,2,3,5},{1,2,4,5},{1,3,4,5},{2,3,4,5},{1,2,3,4,5}}

Para cualquier otro subconjunto de participantes no es posible recuperar la imagen secreta. Por ejemplo, las sombras de {1,3}, {2,4,5} o {1,2,3,4} no recuperarán la imagen original.

A modo de ejemplo, en la figura 3 (tomada de [St95]) puede verse un esquema visual de 4 participantes, {1,2,3,4}, cuyos participantes cualificados elementales son {1,2}, {2,3} y {3,4}. Se observa que la unión de las sombras de {1,3}, {2,4} o {1,4} no recuperan la imagen, mientras que la superposición de las sombras de {1,2} o {3,4} sí que lo hacen.

Figura 3. Ejemplo de esquema visual selectivo con 4 participantes

## 5. ESQUEMAS CRIPTOGRÁFICOS EXTENDIDOS

Los esquemas criptográficos visuales presentados en la sección anterior pueden ampliarse si se consideran junto con los esquemas visuales subliminales. De esta forma, si a la estructura anterior, en la que dentro del conjunto de participantes hay determinados subconjuntos de participantes cualificados, añadimos la posibilidad de que las sombras que se generen por el director contengan imágenes inocentes, estamos ante *los esquemas visuales extendidos* ([BSS99] y [ABSS99]). Por tanto, en este tipo de esquemas se pueden elegir las imágenes que aparecerán en cada una de las sombras de modo que cada participante reconozca cuál le pertenece porque en la misma aparece, por ejemplo, su inicial.

A modo de ejemplo se puede considerar un esquema visual extendido con 3 participantes, {A,B,C}, de modo que los participantes cualificados elementales sean: {A,B} y {B,C}, es decir, $Q$ = {{A,B},{B,C},{A,B,C}}.

En este caso, las sombras que corresponden a los tres participantes podrían ser las de la figura 4 (tomada de [ABSS99]). Como se puede apreciar, cada una de las sombras contiene como imagen inocente una letra: A, B o C, esto es, la inicial de cada participante. A la hora de recuperar la imagen original se aprecia que la superposición de las sombras de participantes cualificados proporciona la imagen original (la letra S); mientras que de las sombras de los participantes no cualificados {A,C} sólo se obtiene la superposición de sus iniciales.

Figura 4. Ejemplo de esquema visual extendido

## 6. SOBRE EL CONTRASTE DE LOS ESQUEMAS VISUALES

En algunos párrafos precedentes se ha comentado, muy de pasada, que cuando se superponen dos o más transparencias, correspondientes a otras tantas sombras, para obtener la imagen original, se produce una pérdida de contraste con relación a la imagen original debido a que los píxeles negros se recuperan como píxeles totalmente negros, mientras que los píxeles blancos se recuperan como grises (mitad blancos, mitad negros en el caso de los esquemas con contraste de pixel $m = 2$). Esta concepción de contraste no contempla otros problemas como pueden ser la pérdida de nitidez de la imagen recuperada por la distorsión que puedan sufrir las transparencias debidas al calor de la impresora o fotocopiadora, cuando se elaboran, etc.

Desde este punto de vista, se puede definir el contraste en un esquema visual como la diferencia entre el nivel de gris de un pixel negro y un pixel blanco. Resulta claro que en los esquemas 2 de 2 presentados, donde el cifrado se lleva a cabo pixel a pixel, y donde cada pixel se cifra por medio de dos píxeles, el mejor contraste que se puede obtener es 0'5. Naor y Shamir ([NS95]) mostraron que en el caso de considerar un esquema visual $t$ de $t$, el mejor contraste que se puede conseguir superponiendo $t$ transparencias o sombras es $1/2^{t-1}$. Posteriormente, los mismos autores ([NS96]) han determinado límites más ajustados para el contraste de este tipo de esquemas como función de la complejidad del esquema, que en este caso se traduce en el número de transparencias superpuestas. El método que utilizan para recuperar una imagen secreta no es exactamente el mismo que el que propusieron inicialmente y que se ha presentado aquí.

El nuevo método de recuperación se basa en lo que los autores llaman *el semigrupo de superposición* ("cover"), cuyos elementos son 2 colores cualesquiera, por ejemplo, el azul (A) y el rojo (R) y por el color "transparente" (T), es decir, el semigrupo es: {A,R,T}. La operación de este semigrupo consiste en la superposición de dos de sus elementos y se presenta en la siguiente tabla:

| **Arriba**<br>**Abajo** | **A** | **R** | **T** |
|---|---|---|---|
| **A** | A | R | A |
| **R** | A | R | R |
| **T** | A | R | T |

Como se puede observar, la operación del semigrupo no es conmutativa, es decir, al superponer un color sobre otro, el resultado es el color que está encima, salvo que éste sea transparente, en cuyo caso, el resultado es, obviamente, el color inferior.

Con este modelo se puede obtener un mejor contraste que con el modelo precedente. El mejor valor del contraste en esta situación es $1-1/c$, siendo $c$ tanto el número de sombras que se superponen como el número de subpíxeles que forman cada uno de los píxeles cifrados. Sin embargo, este nuevo método de recuperación no es aplicable para esquemas visuales umbrales $t$ de $n$ para los que $n \geq t \geq 3$.

En [ES99] se analizan las diferentes propuestas sobre el concepto de contraste y se propone una definición alternativa, presentándose ejemplos de los diferentes contrastes que se pueden conseguir.

## 7. ESQUEMAS VISUALES EN COLOR

Desde la aparición de las primeras propuestas de la criptografía visual y de las extensiones presentadas hasta aquí, queda pendiente la posibilidad de añadir color, tanto a la imagen a cifrar como a las sombras y a la imagen recuperada. De los esquemas planteados se aprecia la dificultad de diseñar criptosistemas visuales en color; sin embargo, se han hecho varias aproximaciones a esta posibilidad ([N94], [RP96] y [VeTi97]). Naccache ([N94]) utilizó el hecho de que cada color se caracteriza por su longitud de onda para proponer el uso de filtros que permitan pasar sólo la luz entre determinados valores de la longitud de onda. El esquema que propuso utiliza dos filtros de modo que la combinación de ambos absorba todas las longitudes de onda excepto la correspondiente al color del dibujo original.

Verheul y van Tilborg ([VeTi97]) describieron un esquema para cifrar imágenes en color. El método para colorear un esquema 2 de 2, por ejemplo, con *r* colores consiste en dividir cada pixel en *r* subpíxeles y cada subpixel es dividido en *r* regiones, una región fija para cada color. De esta manera, si el color del pixel original es *c*, la región del subpixel correspondiente a ese color tendrá el color *c* (se dirá que el subpixel es de color *c*) mientras que el resto de las regiones tendrá color negro. Una vez definido el esquema, a la hora de superponer las sombras se obtienen píxeles negros excepto cuando los dos subpíxeles son del mismo color, es decir, tienen en la misma región el mismo color. Para cifrar un pixel de color *c* hay que asegurarse que los subpíxeles de color *c* tienen la misma posición en ambas sombras y que esto no se verifica para ningún otro color. Una desventaja clara de este esquema es que hay una gran pérdida de contraste, puesto que si se desea cifrar un imagen que tenga *r* colores se obtiene una reducción en la resolución de un factor $r^2$.

En la figura 5 se pueden observar los píxeles para dos sombras de modo que cifren píxeles en color. Se presenta también una imagen sencilla coloreada, sus sombras y la recuperación de la misma. La imagen original, de tamaño 12×12 píxeles se presenta sólo a título de ejemplo, por lo que la resolución de la misma está claramente aumentada. Como se puede observar, la imagen original sólo tiene cuatro colores: negro, rojo, verde y azul. Para cifrar cada uno de los píxeles en color originales, se considera que el fondo de la imagen es negro, por lo que los colores que en realidad se deben cifrar son sólo tres: rojo, verde y azul. Por esta razón, cada uno de los píxeles cifrantes se divide en 3 subpíxeles horizontales y cada uno de los subpíxeles es dividido en 3 regiones ordenadas: la primera es para el color rojo, la segunda para el verde y la tercera para el azul. En la figura 5 se observa un ejemplo de cómo se puede cifrar un pixel original negro, uno rojo, uno verde y uno azul. Nótese la pérdida de color de la imagen recuperada comparada con la imagen original.

Figura 5. Píxeles en color y ejemplo de imagen en color cifrada y recuperada

Una solución diferente para imágenes en color y esquemas visuales 2 de 2 se plantea en [RP96]. En este caso, cuando se superponen dos colores diferentes se obtiene un tercer color: la suma de los dos anteriores. Por ejemplo, la superposición de rojo (R) y verde (V) da amarillo. Así, la combinación de los tres colores básicos, Rojo, Verde y Azul, proporciona los colores que se muestran en la siguiente tabla:

| **Color** | **Rojo** | **Verde** | **Azul** |
|---|---|---|---|
| **Rojo** | Rojo | amarillo | Morado |
| **Verde** | amarillo | Verde | Cian |
| **Azul** | Morado | Cian | Azul |

Si este procedimiento puede resultar difícil a la hora de superponer dos transparencias porque los colores no se suman y uno de ellos “tapa” al otro, el remedio puede consistir en utilizar alguno de los muchos programas de dibujo que existen en el mercado y que permiten “sumar” los colores de dos imágenes recurriendo a sistema RGB (Red, Green y Blue).

La solución propuesta por Rijmen y Preneel consiste en dividir cada pixel en cuatro subpíxeles con los colores básicos anteriores: rojo, verde, azul y blanco, de modo que dichos colores pueden aparecer en cualquier orden. Superponiendo dos píxeles divididos en los cuatro subpíxeles anteriores de todas las formas posibles y considerando las posibles

simetrías, se obtienen 24 píxeles básicos, es decir, 24 colores si cada uno de los píxeles resultantes se empareja con el color que más se le parezca, en función de los colores de los subpíxeles que le forman.

Una vez planteada la anterior situación, para cifrar un pixel de un color determinado de la imagen original se selecciona el pixel coloreado de los 24 anteriores cuyo color más se aproxima al color original. A continuación se selecciona un orden aleatorio para los subpíxeles de la primera sombra y se selecciona el orden de los subpíxeles para la segunda sombra de modo que su unión produzca el color requerido. La ventaja de este esquema es que permite representar 24 colores con una reducción en la resolución de un factor 4 en lugar del factor $24^2$ como sería en el caso de utilizar el método propuesto por Verheul y van Tilborg. Un inconveniente de este método es que una vez fijados los colores de los subpíxeles, quedan determinados los 24 colores iniciales. Este esquema se puede extender a más colores sin más que dividir cada pixel en un número mayor de subpíxeles.

## 8. AUTENTICACIÓN E IDENTIFICACIÓN VISUAL

Los problemas de autenticación e identificación han recibido un gran interés en criptografía. En la actualidad es uno de los campos de investigación más interesantes debido, fundamentalmente, a la proliferación de tarjetas de pago y monederos electrónicos. En estos contextos se hace necesaria la autenticación e identificación del propietario de la tarjeta y sería interesante disponer de algún sistema que, sin utilizar dispositivos computacionales complicados, llevara a cabo este objetivo.

Recordemos que en un protocolo de autenticación, un *remitente* intenta transmitir un mensaje a un *destinatario* mientras un *adversario* controla el canal de comunicación que es utilizado. Al final del protocolo, el destinatario debe ser capaz de determinar si el mensaje que ha recibido es el mismo que el que le fue enviado por el remitente o si ha sido modificado por el adversario durante el protocolo. Por su parte, en un protocolo de identificación, un *usuario* tiene que probar su identidad ante un *verificador*, de modo que un *adversario* no sea capaz de suplantar al usuario y engañar al verificador.

En [NP97] se presenta un escenario en el que se hace uso de lo que se ha venido en llamar “baja tecnología”, de modo que tanto el destinatario del protocolo de autenticación como el usuario en el protocolo de identificación son humanos (no ordenadores) y no pueden llevar a cabo cálculos complicados ni almacenar una excesiva cantidad de datos. En este escenario se hace uso de la criptografía visual y se define la *autenticación visual y la identificación visual*. Con ello se trata de proponer una alternativa a los métodos clásicos de autenticación e identificación, de modo que no se haga uso de “alta tecnología”.

Siguiendo la tradición de la criptografía, en estos esquemas consideraremos el recipiente Horacio, *H*, (dado que es un Humano con pocos recursos tecnológicos y no un ordenador), el informante Teresa, *T*, (dado que a menudo el informante es una Tarjeta) y el adversario Pilar, *P*, (porque en algunas aplicaciones el adversario es el Punto de venta).

Los *esquemas de autenticación* propuestos en [NP97] hacen uso de baja tecnología y son seguros contra un adversario con ilimitada potencia de cálculo y memoria. Además, los cálculos y requerimientos de memoria necesarios para *T* son lineales en el tamaño del mensaje y están dentro de la potencia actual de computación de las tarjetas electrónicas. En los esquemas de autenticación visual, *T* produce una cadena aleatoria *r*, crea una transparencia $T_r$ y alguna información auxiliar $A_r$ que es función de *r*. En estos esquemas *T* desea comunicar a *H* una información *m*, el contenido de la cual es conocido por *P* y sigue el siguiente *protocolo de autenticación*:

1. *T* envía un mensaje *c* a *H*, que es una función de *m* y de *r*.
2. *P* puede cambiar el mensaje *c* antes de que *H* lo reciba.
3. Una vez que *H* ha recibido el mensaje *c*’ su repuesta es «RECHAZO» o «ACEPTO *m*’» como función de *c*’ y su información secreta $T_r$ y $A_r$. Si la respuesta es «ACEPTO», también envía a *T* el valor de *m*’, la información que *H* cree recibir de *T*.

En este modelo, el adversario *P* puede cambiar el mensaje que *T* envía a *H* en la forma que desee, sin embargo, en un esquema visual, toda sombra legal debería contener exactamente dos subpíxeles negros en cada pixel cuadrado de tamaño 2×2. Entonces, *P* podría llevar a cabo dos tipos de cambios. El primero de ellos consistiría en cambiar la posición de dos subpíxeles negros en los píxeles de la imagen, cambio que no sería detectado por *H*. El segundo cambio podría ser el de colocar más de dos subpíxeles negros en cada pixel cuadrado original, lo que produciría una sombra ilegal del esquema visual. Sin embargo, esta modificación es difícilmente detectable por *H* (recuérdese que *H* es humano) a no ser que el cambio sea hecho en muchos pixeles.

A modo de ejemplo, presentaremos una situación de comercio electrónico en la que la autenticación visual puede proteger contra un posible intento de fraude. Supongamos un escenario de pago con tarjeta electrónica. Horacio, un cliente, tiene su tarjeta monedero electrónico que contiene determinada cantidad de dinero. Horacio quiere comprar algo a Pilar y pagar con su tarjeta, para lo cual se debe llevar a cabo un proceso de transacción entre la tarjeta de Horacio y el punto de venta de Pilar, después del cual, determinada cantidad de dinero ha sido transferida desde la tarjeta a Pilar. Las tarjetas monedero comunes no tienen un dispositivo que permita mostrar o recibir directamente información y todas las entradas y salidas de la transacción se llevan a cabo mediante un servidor remoto. Una traducción literal de esta situación en una compra-venta normal sería que el vendedor tomara el monedero del comprador y se sirviera él mismo de la cantidad correspondiente al importe de la compra (la mayor parte de los clientes no aceptarían esta forma de pago).

Supongamos el siguiente intento de fraude por parte de Pilar, que aún no ha recibido una solución aplicable para las tarjetas de pago estándar. Horacio compra algo por un importe de 1 euro. Pilar pide a la tarjeta de Horacio, *T*, que pague una cantidad de dinero, por ejemplo 10 euros. La tarjeta podría pedir a Horacio conformidad de la cantidad solicitada, pero toda comunicación entre Horacio y su tarjeta pasa por Pilar, quien podría cambiar los contenidos. Sería preferible que Horacio pudiera enviar a su tarjeta una conformidad que fuera función del importe a pagar y de alguna información secreta que sólo su tarjeta conociera. Sin embargo, esta situación es difícil dado que Horacio es humano (no un ordenador) y no tiene capacidad para llevar a cabo cómputos complicados. Este problema se resolvería permitiendo una comunicación fiable entre Horacio y su tarjeta mediante autenticación visual. La tarjeta podría enviar a Horacio la suma que se le pide que pague y Horacio podría responder con su aprobación o su rechazo mediante un determinado password que sólo los dos conocieran.

Los escenarios para la *identificación visual* son muy similares a los de autenticación visual, como ya se ha mencionado antes. Sin embargo, el objetivo del protocolo de identificación visual es diferente: se trata de permitir a un usuario humano, *H*, probar su identidad ante un verificador, *T*, sin necesidad de consultar ningún dispositivo de computación. El objetivo de adversario, *P*, es convencer al verificar de que ella, Pilar, es el usuario. El protocolo de identificación visual es del tipo desafío-respuesta en el que el verificador, Teresa, envía al usuario un desafío, quien debe responder al mismo en base a algún tipo de información secreta que él (Horacio) posee.

El *protocolo de identificación* de *H* a *T* en la etapa *i*-ésima es el siguiente:

1. *T* envía a *H* un desafío $d_i$, que es función del dato secreto *r*.
2. Una vez recibido $d_i$, el usuario humano calcula una respuesta $r_i$ como función de $d_i$ y su información secreta $T_r$ y $A_r$, y se la envía a *T*.
3. *T* decide si la otra parte es *H* o no, teniendo en cuenta $d_i$ y $r_i$ y el dato secreto *r*. Entonces *T* responde «ACEPTO» o «RECHAZO».

En los métodos de identificación propuestos en [NP97] no se hace uso de esquemas visuales umbrales 2 de 2, como en los esquemas de autenticación visual. En aquellos se tiene en cuenta que *H* debe probar a *T* que conoce alguna propiedad de la transparencia. Además, es posible utilizar transparencias con 10 colores, que son fácilmente discernibles entre sí. Por otra parte, dado que la navegación en Internet mediante “world-wide-web” ha

introducido un interfaz gráfico estándar universal, es posible utilizar estos métodos de identificación cuando un usuario se conecta con un ordenador remoto mediante un navegador web. Para ello bastaría con presentar en la pantalla del usuario una imagen generada por el verificador. Téngase en cuenta que con este procedimiento no haría falta instalar nuevos programas en el ordenador remoto para la identificación. Además, el trabajo del verificador sería muy poco y los papeles del usuario y verificador serían reversibles.

**Referencias:**


[ABSS96] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R. *Visual cryptography for general access structures*. Information and Computation 129, 1996, pp. 86-106.

[ABSS99] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R. *Extended capabilities for visual cryptography*. Por aparecer en Theoretical Computer Science.

[BSS99] Blundo, C., De Santis, A. and Stinson, D. R. *On the contrast in visual cryptography schemes*. Journal of Cryptology v. 12, n. 4, 1999, pp. 261-289.

[ES99] Eisen, P. A. y Stinson, D. R. *Threshold visual cryptography schemes with specified whitness levels of reconstructed pixels*. Disponible en http://cacr.math.uwaterloo.ca/dstinson/

[FGHMM97] Fúster Sabater, A., De La Guía Martínez, D., Hernández Encinas, L., Montoya Vitini, F. y Muñoz Masqué, J. *Técnicas criptográficas de protección de datos*. RA-MA, Madrid, 1997.

[HM99] Hernández Encinas, L. y Minguet Melián, J. *Criptografía visual*. Novática, 138, 1999, pp. 63-68.

[N94] Naccache, D. *Colorful cryptography –a purely physical secret-sharing scheme based on chromatic filters–*. Coding and Information Integrity, French-Israeli workshop, 1994.

[NP97] Naor, M. and Pinkas, B. *Visual authentication and identification*. Advances in Cryptology-CRYPTO'97. LNCS 1294, 1997, pp. 322-336.

[NS95] Naor, M. and Shamir, A. *Visual cryptography*. Advanced in Cryptology, EUROCRYPT'94, LNCS 950, 1995, pp. 1-12.

[NS96] Naor, M. and Shamir, A. *Visual cryptography II: Improving the contrast via the cover base*. Theory of Cryptography Library, report 96-07. Disponible en ftp://theory.lcs.mit.edu/pub/tcryptol/96-07.ps.

[RP96] Rijmen, V. and Preneel, B. *Efficient colour visual encryption or "Shared colors of Benetton"*, presentado en EUROCRYPT'96, Rump session. Disponible en htpp://www.iacr.org/conferences/ec96/rump/preneel.ps

[St95] Stinson, D. R. *An introduction to visual cryptography*. Comunicación personal.

[VeTi97] Verheul, E. R. and van Tilborg, H. C. A. *Constructions and properties of k out of n visual secret sharing schemes*. Designs, Codes and Cryptography 11, 1997, pp. 179-196.

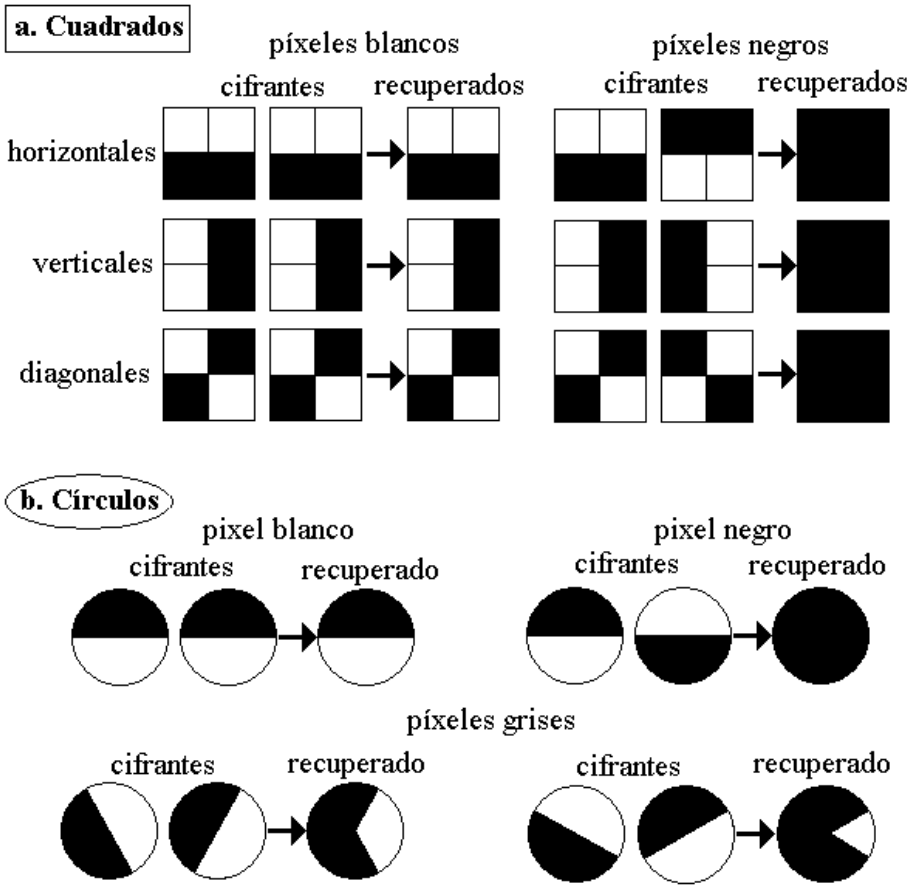
a. Cuadrados
píxeles blancos
cifrantes
recuperados
píxeles negros
cifrantes
recuperados
horizontales
verticales
diagonales
b. Círculos
pixel blanco
cifrantes
recuperado
pixel negro
cifrantes
recuperado
píxeles grises
cifrantes
recuperado
cifrantes
recuperado

Figura 1

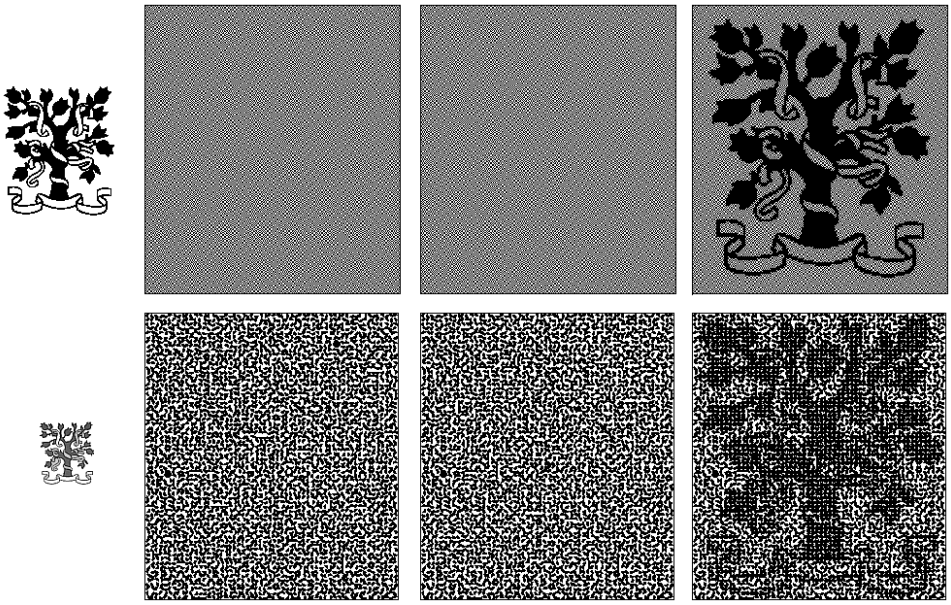

Figura 2

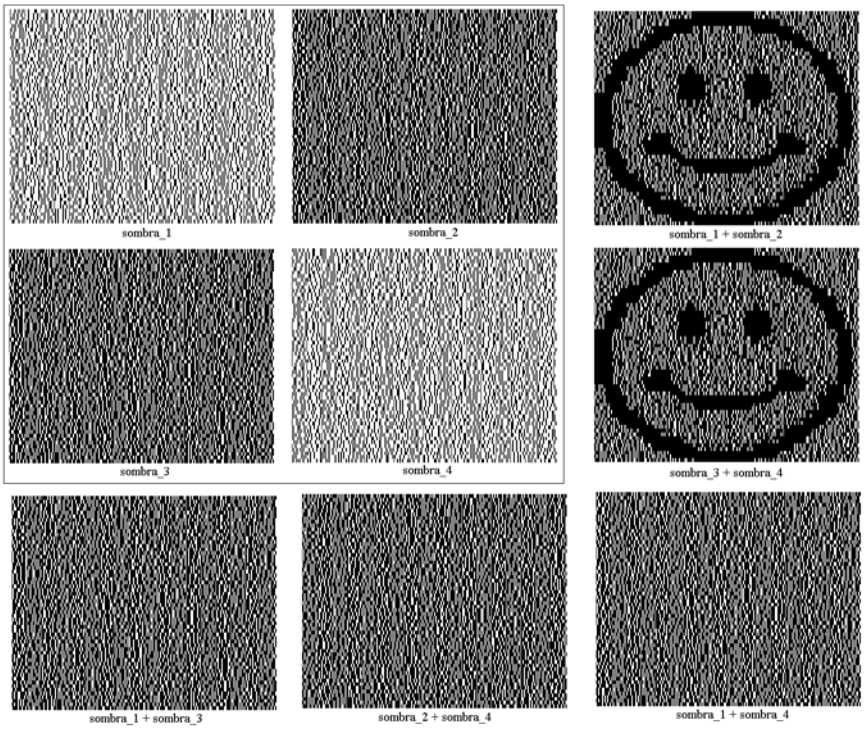
sombra_1
sombra_2
sombra_1 + sombra_2
sombra_3
sombra_4
sombra_3 + sombra_4
sombra_1 + sombra_3
sombra_2 + sombra_4
sombra_1 + sombra_4

Figura 3

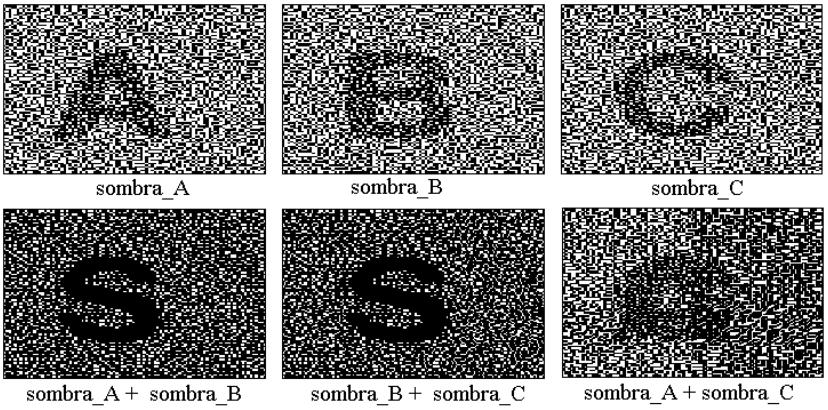
sombra_A
sombra_B
sombra_C
sombra_A + sombra_B
sombra_B + sombra_C
sombra_A + sombra_C

Figura 4

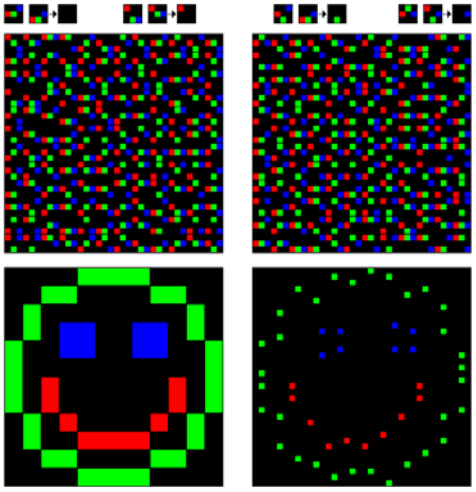

Figura 5